WHAT IS CLAIMED IS:

1. A method for encrypting digital data, comprising:

decrypting digital data which has been encrypted at a high encryption level;

storing a predetermined amount of the decrypted digital data in a buffer;

reencrypting digital data output from the buffer at a low encryption level; and

transferring the reencrypted digital data to a digital data player or a data storage medium.

2. The method as set forth in claim 1, wherein the storing step includes

variably setting an effective capacity of the buffer according to a size of the digital data.

3. The method as set forth in claim 2, wherein the effective capacity of the buffer is smaller than the size of the digital data.

4. The method as set forth in claim 1, wherein the reencrypting step includes

encrypting certain portions of the decrypted digital data, thereby leaving decrypted remaining portions of the decrypted digital data in the reencrypted digital data.

5. The method as set forth in claim 1, wherein the reencrypting step includes

weakly encrypting all of the decrypted digital data.

6. A method for encrypting digital data, comprising:

determining whether digital data which has been encrypted at a high encryption level must be protected from unauthorized copying;

decrypting the digital data; and

reencrypting the decrypted digital data at a low encryption level if the decrypted digital data must be protected from unauthorized copying.

7. The method as set forth in claim 6, wherein the reencrypting step includes

encrypting certain portions of the decrypted digital data, thereby leaving

decrypted remaining portions of the decrypted digital data.

8. The method as set forth in claim 6, wherein the reencrypting step includes weakly encrypting all of the decrypted digital data.

9. The method as set forth in claim 6, further comprising

storing a predetermined amount of the decrypted digital data in a buffer prior to the reencrypting step if the decrypted digital data must be protected from unauthorized copying.

10. A method for encrypting digital data, comprising:

determining whether digital data which has been encrypted at a high encryption level must be protected from unauthorized copying;

decrypting the digital data; and

transferring the decrypted digital data to a digital data player or a data storage medium if the decrypted digital data need not be protected from unauthorized copying.

11. The method as set forth in claim 10, further comprising

reencrypting the decrypted digital data at a low encryption level if the decrypted digital data must be protected from unauthorized copying.

12. A program (or script) embodied on a computer-readable medium for encrypting or decrypting a digital data file, the computer-readable-medium-embodied program comprising:

a first program code segment to receive and store digital data encrypted to a high level and an encryption key;

a second program code segment to decrypt the stored digital data using the encryption key;

a third program code segment to store a predetermined amount of the decrypted digital data in a buffer; and

a fourth program code segment to reencrypt the digital data from the buffer to a low level and download the reencrypted digital data to a digital data player or a data

storage medium.


0047620 "02/25/00